This Chapter has been rescinded by VHA Directive 6210

http://vaww.va.gov/publ/direc/health/direct/vha6210d.pdf

Department of Veterans Affairs
Veterans Health Administration
Washington, DC 20420

M-11
Chapter 16

January 17, 1995

1. Transmitted is a new chapter to the Department of Veterans Affairs, Veterans Health Administration (VHA) Manual, M-11, "Information Resources Management," Chapter 16, "Automated Information System (AIS) Security."

2. Chapter 16 provides policy and procedures to ensure the protection of data, hardware, software, and storage media.

3. **Filing Instructions**

Remove pages	**Insert pages**
	16-i
	16-1 through 16-22
	16A-1 through 16A-3

4. **RESCISSIONS:** VHA Circulars/Directives 10-85-93, 10-85-112, 10-85-116, 10-86-147, 10-87-19, 10-87-119, 10-87-122, and 10-87-123.

Kenneth W. Kizer, M.D., M.P.H.
Under Secretary for Health

Distribution: **RPC 1476 is assigned.**
FD

Printing Date: 1/95

CONTENTS

CHAPTER 16. AUTOMATED INFORMATION SYSTEM (AIS) SECURITY

CHAPTER 16. AUTOMATED INFORMATION SYSTEM (AIS) SECURITY

16.01 PURPOSE

a. The purpose of information security is to ensure:

(1) Data integrity;

(2) System reliability and operational availability;

(3) Authorized data access;

(4) Proper disclosure; and

(5) Protection of hardware, software and storage media.

b. This chapter provides Department of Veterans Affairs (VA) Veterans Health Administration (VHA) information security policy and procedures for all VHA elements such as VHA health care facilities, Information Systems Centers (ISCs) and field components of VA Central Office.

c. The procedures described in this chapter serve as the VHA AIS Security Manual for those persons responsible for managing, coordinating, and implementing the VHA AIS Security Program. These persons include:

(1) The facility Director and management down to the unit supervisors;

(2) The Information Security Officer (ISO), alternate ISO and designees;

(3) Information Resource Management (IRM) personnel;

(4) Regional ISO (RISO); and

(5) VHA Central Office staff.

d. This chapter describes the program under which VHA shall implement the requirements of VA policy concerning the safeguarding of all information assets at all VHA facilities and offices and encompasses all computer systems operating therein. Maintaining the quality of data remains the responsibility of the individuals having input and access to the databases.

e. This chapter provides references to procedures for the management of all facets of an Information Security Program such as personnel security management, security awareness, system access (both physical and logical), risk analysis, contingency planning, and procedures for handling breaches of security.

NOTE: *Specific information security procedures shall be the responsibility of the organizational elements responsible for each area addressed in this chapter.*

16.02 POLICY

a. VA AIS Security Policy, MP-6, Part I, Chapter 2, established policies and responsibilities for information security within VA and provides a structure for implementing the requirements of the Office of

Management and Budget (OMB) Circular A-130 and other Federal information security laws and regulations (see App. 16A).

b. In compliance with the intent of OMB Circulars A-123, A-127, and A-130, and the Privacy Act of 1974, VHA established a comprehensive information security program. This program provides for the adequate safeguards of sensitive data processed by automated systems in all VHA facilities, offices, and in leased facilities.

16.03 DEFINITIONS

a. **Access.** Access is the ability and the means necessary to locate, store, delete, or retrieve data, text and images, and to communicate with or to make use of IRM resources and system functional privileges.

b. **Access Code(s).** Access codes are the code(s) assigned by the Chief, IRM Service, to uniquely identify each individual user. For Decentralized Hospital Computer Program (DHCP) this code should be a string of a least six characters paired with a verify code.

c. **Accreditation.** Accreditation is the management authorization and approval granted to an AIS to process sensitive data based upon the results of certification.

d**. AIS.** AIS is an assembly of computer hardware and software configured for the purpose of classifying, sorting, calculating, summarizing, transmitting and receiving, storing and retrieving data with a minimum of human intervention.

e. **Audit Trail and/or Logging Features.** These features are automated software procedures to help:

(1) Maintain the integrity of the system and database.

(2) Determine whether the security controls implemented for protection of computer system resources are being circumvented.

(3) Identify the potential source(s) of security breaches.

f. **Certification.** Certification is an evaluation made in support of the accreditation process that establishes the extent to which an existing sensitive AIS meets a pre-specified set of security requirements.

g. **Data and/or Information Security.** Data and/or information security is the protection of data and/or information from accidental or malicious modification, destruction, disclosure or denial, specifically addressing data access mechanisms, electronic transmission of data and/or information, and identification and protection of storage devices used to store sensitive data.

h**. Double Envelope Method.** The double envelope method is a procedure which involves the transmittal of security codes and sensitive documents which are sealed in the inner of two envelopes. Both envelopes shall be addressed to the recipient. The inner envelope shall also display the name and address of the sender, the statement "TO BE OPENED BY ADDRESSEE ONLY" and instructions for contacting the local ISO if it is found to be opened upon receipt. The outer envelope shall also be sealed.

i. **Information Security Incident.** An information security incident is any situation either natural or man made that leaves an information system in a less than fully operational state or which violates AIS security-related laws or policies (e.g., fraud, virus infection, disclosure, hacking, hurricane), thereby either creating the potential for the destruction or compromise of VHA data, or actually causing the destruction or compromise of VHA information.

j. **National Center for Information Security (NCIS).** The NCIS facility, which is adjunct staff to the VHA ISO, is located at the VA Medical Center, Martinsburg, WV, and is staffed with specialists in information security. The previous name of the facility was the National Center for Automated Data Processing (ADP) Security.

k. Personnel Security. Personnel security consists of procedures established to ensure that all personnel who have access to any sensitive computer material have the required authorization as well as all appropriate clearances.

l. **Physical Security.** Physical security consists of the use of doors, walls, locks, guards, badges, and similar measures to control access to the computer and related equipment, and the measures required for the protection of the structures housing the computer, related equipment, and their contents from damage by accident, fire, environmental hazards and malicious actions.

m. **Residual Risk.** Residual risk is the remaining risk to a sensitive AIS after controls are established to counter threats.

n**. Risk Analysis.** Risk analysis is an analysis of system assets and vulnerabilities to establish an expected loss from certain events based on estimated probabilities of the occurrence of these events.

o. **RISO.** The RISO is the security specialist who participates in the development of the VHA national information security program and assists regional facilities in the implementation of local security programs. The RISO is located at an ISC.

p. **Security Code.** A security code is a string of numeric or alphanumeric characters that uniquely identifies an authorized user to a host computer and permits system access.

q**. Sensitive Data and/or Text and/or Images.** Sensitive Data/Text/Images is material that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, denial, or destruction. Improper use or disclosure of such material could adversely affect the ability of an agency to accomplish its mission such as proprietary data, records about individuals requiring protection under the Privacy Act of 1974, and/or other confidentiality statutes. This definition includes sensitive information as set forth in 15 United States Code (U.S.C.) 278g-3-(d) (4), as amended by Section 3 of the Computer Security Act of 1987, Public Law No. 100-235, 101 Stat. 1724, 1727 (1988).

r. **System of Records.** The term "system of records" means a group of any records under the control of the Department from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

s. **Telecommunications and Networks**

(1) Telecommunications refers to any transmission, emission, or reception of signs, signals, writing, images, sounds, or information of any nature, by wire, radio, visual, or other electromagnetic systems.

(2) Networks fall within the realm of telecommunications and consist of any interconnection of computers and terminals via communications lines. Sensitive information on networks may be vulnerable to disclosure through manipulation of network interfaces or components, both intentionally and by accident.

16.04 RESPONSIBILITIES

a. The Director, Medical Information Resources Management Office (MIRMO), has overall program responsibility for the VHA AIS Security Program and ensures that development and implementation of the AIS Security Program meets all Federal, Departmental, and VHA standards, policies and guidelines.

b. The Director, Medical Information Security Service (MISS), MIRMO, is the VHA ISO responsible for the following functions:

(1) Developing and disseminating AIS security policy and guidelines to support the implementation of an effective national information security program in all VHA offices and facilities which use computing resources.

(2) Assisting with office and facility management of information security activities, as requested.

(3) Providing oversight of VHA AIS security incident program and reports such events as required.

(4) Reviewing and disseminating information and implementing procedures on:

(a) New laws, regulations, and VA and VHA policies concerning information security;

(b) New technology and techniques to improve information security measures;

(c) Investigation of criminal information security breaches;

(d) Security awareness activities and training as set forth in the Office of Personnel Management (OPM) Computer Security Training guidance; and

(e) Ensuring OMB required certification documents are created/renewed for centrally-managed systems (e.g., DHCP).

c. The RISO is an adjunct position to the VHA ISO and is located at an ISC as a base of operations. The RISO is responsible for and participates in the development of the VHA National Information Security Program and assists regional facilities with their local AIS security programs.

d. The Director of each health care facility is responsible for the implementation of the corresponding facility Information Security Program and shall be responsive to the procedures provided. Each facility Director shall designate an ISO whose responsibility will be the development, implementation, and monitoring of station-specific information security policy and procedures. This responsibility should be assigned to an individual knowledgeable in information technology and security matters. It is desirable from a security standpoint that key positions be separated so that the duties of any one person will not adversely affect the AIS due to conflict of interest or malicious intent.

e. The facility ISO is the principal officer at a VHA health care facility responsible for:

(1) Ensuring that policies and procedures related to the availability and integrity of all sensitive data in all information systems at the facility are in place and adhered to;

(2) The management and coordination of an information security program which is in compliance with this chapter and with other official documents which address the specific organizational structure, physical environment, and computing resources of the facility or office; and

(3) Security training and ensuring that risk analyses are conducted at the facility.

f. The health care facility Chief, IRM Service, is responsible for:

(1) Implementing security procedures at the facility;

(2) Ensuring adequate security access is limited to authorized users;

(3) Establishing procedures to ensure data required for contingency planning is current;

(4) Ensuring that a satisfactory preventive maintenance schedule is established;

(5) Maintaining accountability for the facility systems as outlined in the VHA security program; and

(6) Making recommendations to the Director, MISS, for any changes in the security program.

g. All users who have access to sensitive automated information systems are responsible for compliance with AIS security requirements. The quality, confidentiality, and integrity of data are the responsibility of all users of AIS in accordance with MP-6.

16.05 PROCEDURES FOR PERSONNEL SECURITY MANAGEMENT

a. The Federal Personnel Manual (FPM), Chapter 731, establishes policy for personnel suitability. Procedures for designation of position sensitivity levels with respect to suitability shall be in accordance with FPM Chapter 731 and MP-6, Chapter 2. FPM, Chapter 732, establishes policy for personnel security. Procedures for designation of position sensitivity levels for positions that have National Security duties shall be in accordance with FPM Chapter 732.

(1) Facility directors shall ensure that all positions are assigned a proper sensitivity level designation based on information security criteria, such as computer-related responsibilities, type of data the individual has access to, a reasonable analysis of the risk, and principles of responsible management.

(2) Field management shall evaluate, at a minimum, the following positions for the proper sensitivity level designation; these positions shall be designated no lower than moderate risk (level 5C), and include:

(a) Facility ISO(s) and alternates,

(b) IRM staff (excluding clerical positions),

(c) Quality Assurance Coordinator, and

(d) Chief, Fiscal Service.

(e) Individuals having either programmer privileges or the ability to create and add users and/or menus or establish file access for computer systems which process sensitive data.

b. Service chiefs with assistance from ISO and Human Resources Management chiefs shall analyze all positions, establish their sensitivity level designation, and document them with VA Form 50-2280, Position Sensitivity Level Designation. VA Form 50-2280 shall be signed by either the facility Director, or designee (e.g., Chief, Human Resources Management).

c. **Documentation of Information Security Responsibilities**

(1) **Position Descriptions**. Position descriptions shall be written or annotated to reflect specific security responsibilities and position sensitivity levels. Within this context, "specific security responsibilities" refer to employee obligations to protect sensitive data and to use such data and information derived from it only in the execution of official duties.

(2) **Supervisor Responsibilities**

(a) The supervisor of the employee shall review annually the position description and performance standards with each employee occupying a position designated as sensitive.

(b) The supervisor and employee shall discuss specific information security responsibilities.

(c) Consequences of noncompliance with those security responsibilities for the particular position shall be outlined for the employee.

d. **Incidents**

(1) Each VHA facility shall establish procedures within its facility security plan for reporting information security incidents.

(2) Due to the possible critical threat information security incidents pose, communication channels will be selected to provide confidentiality and will be commensurate with the security violation. Detailed written accounts of the incident shall be considered sensitive and mailed directly to the higher authorities using the double envelope method and express mail. All information of the incidents shall be considered sensitive and kept in a secured area.

(3) Procedures shall address the following minimal reporting requirements:

(a) How incidents should be reported and the communication channels to be followed,

(b) Employee responsibilities for reporting incidents,

(c) Management responsibilities in responding to incidents,

(d) Incorporation of an incident reporting program into employee information security awareness training,

(e) Establishment of incident reporting procedures,

(f) Investigation of reported incidents,

(g) Procedures for actions in response to investigated incidents,

(h) Maintenance of a log of AIS security incidents, and

(i) Procedures for direct calls to higher authorities and for using the double envelope method.

e. **Transfers and/or Terminations.** When an employee in a sensitive position transfers to a non-sensitive position or is separated from the facility, Human Resources Management Service shall notify the Office of Inspector General (OIG) Security Office in writing. Additional guidance on procedures for transfer, termination, or separation of employees is provided in paragraph 16.09, Procedures for User Access.

16.06 PROCEDURES FOR AIS SECURITY AWARENESS

a. The Computer Security Act of 1987, mandates that all Federal agencies provide information security training for staff and other users of sensitive Federal computer systems. The law requires additional user information security training each year. Successful VHA Information Security Programs require staff, trainees, contractors, and volunteers to be knowledgeable about and convinced of the necessity for information security; and to know their specific information security responsibilities.

b. Facility Directors are responsible for ensuring that all applicable staff receive information security training to maintain a general level of awareness of the threats to and vulnerabilities of computer systems and for encouraging the use of improved computer security practices. All new users shall receive

information security training during their orientation processing and ensure that this training is documented.

c. Information security awareness programs should address the:

(1) Definition of information security.

(2) Relationship of information security to the job-related activities of the employee.

(3) Specific responsibilities of each employee, trainee, contractor, and volunteer.

(4) Consequences to the agency, an employee, trainee, contractor, and volunteer for an intentional breach of security.

d. The RISO shall provide assistance and support to the ISOs within their regions. The security awareness programs shall be reviewed during scheduled site visits.

e. The facility ISO shall monitor the Information Security Awareness Program and recommend policy and procedure. Specific information security responsibilities shall be defined for each affected position and consequences of noncompliance to information security procedures shall be implemented according to guidelines provided in MP-5, Part I, Chapters 735 and 752, concerning employee conduct.

f. Information security shall be presented in a positive, cost-effective way and management should participate in orientation and continuing education activities to emphasize their support of the information security program.

g. The facility ISO shall distribute nationally provided security training information to the facility staff as it becomes available and work closely with the unit supervisors to disseminate this information. Facilities are encouraged to supplement national materials with local training material applicable to facility-specific information security.

h. Employees who have functional responsibilities in information security areas (e.g., ISO and the Chief, IRM Service) should be extended the opportunity to attend security training lectures, courses, etc., as work schedules and funding allow.

i. **User Awareness Training**

(1) **Initial Training**

(a) Information security orientation shall be presented by the facility ISO, or designee, during employee entry processing.

(b) The user must understand the basic purpose of the facility Information Security Program and its implementation before AIS access is granted. At a minimum, users must know the:

1. AIS security policy of the facility;

2. Purpose of information security;

3. Identification and role of the facility ISO;

4. Reporting of security concerns to their supervisor; and

5. Basic procedures for ensuring AIS security.

(c) Users should be familiar with good information security practices. Such practices include:

1. Do not share computer passwords (e.g., access and/or verify codes for DHCP) with anyone.

2. Do not display or write computer passwords.

3. Do not use obvious computer passwords such as dates of birth or names of children.

4. Do not smoke, eat, or drink near computer equipment to avoid contamination or damage.

5. Do not use the computer for personal business.

6. Do not leave the terminal on-line when it is unattended.

7. Do not forget to label and secure sensitive data printouts, computer documents, or media.

8. Do not copy copyrighted software packages.

9. Report the presence of unofficial software to supervisor.

(d) Copies of the facility AIS security policy and information security procedures shall be provided to the employee by the supervisor and discussed as they relate to the specific position. The employee shall be asked to review the information and to sign a statement indicating that the policy and procedures are understood.

(2) **Continuing Training**

(a) The user (e.g., employee, trainee, contractor, volunteer) shall receive continuing training annually in additional aspects of information security as it relates to the requirements of the duties of the individual. Training shall be monitored by the ISO and shall address the items listed in subparagraph 16.06c, under Procedures for AIS Security Awareness.

(b) Each employee is required annually to review the station information security policy and/or procedures.

(c) Continued employee training in major AIS Security Program areas includes, but is not limited to:

1. **AIS Security Program Assessment.** Training shall be assessed by the facility ISO and must comply with Information Security Program policy and procedures.

2. **Security of Sensitive Data.** Training shall address the:

a. Definition of sensitive data;

b. Need to protect sensitive data;

c. Sensitivity of the data handled by the position;

d. Procedure for the proper control and disposal of sensitive data;

e. Importance of accuracy, appropriateness, and timeliness of data input;

f. Need to control the manipulation or improper use of data; and

g. Need to maintain the integrity of databases.

3. **User Access.** Training shall address the:

a. Concept of "the lowest level of access required" as it relates to their VHA duties;

b. Confidentiality of individual access/verify/electronic signature codes;

c. Changing of DHCP verify codes at least every 90 days; and

d. Committing of passwords to memory.

4**. Personnel Security Management.** Training for management shall address the clearances and sensitivity level designations of positions and security responsibilities as reflected in position descriptions and performance standards.

5. **AIS Security Awareness.** Training shall address the:

a. Necessity for employee training and/or updates on security procedures;

b. Annual review of security procedures; and

c. Employee Request for AIS.

6. **Technical Security.** Training shall address the:

a. Computer terminal security awareness for each user log-on,

b. Limits on access to data based on least access principles, and

c. Security of peripheral devices and personal computers.

7. **Physical Security.** Training shall address:

a. Security safeguards used at the site (e.g., locked doors, limits on access, badges);

b. Procedures for fire, vandalism, accident, other environmental hazards; and

c. Procedures and controls for taking equipment, software, and data storage media off station.

(3) As the position of an employee changes or is revised, the need for appropriate information security training shall be assessed by the supervisor. Employees should be solicited for ideas on how to improve information security in the facility. Everyone should be encouraged to view information security as a positive procedural tool, not as an obstacle. Use of posters and occasional videos are encouraged to promote information security awareness.

16.07 PROCEDURES FOR SECURITY OF SENSITIVE DATA

Guidelines have been provided by law, Federal regulations, and VA statutes, specifically including VA confidentiality statutes, which define the sensitivity of data and information (see App. 16A). According to these guidelines, certain types of data processed by VHA computers are considered sensitive. Each VHA facility is responsible for designating the sensitivity of the data and/or information under its administrative control. Examples of sensitive material processed by VHA computer systems are listed as follows:

a. **Categories of Data**

(1) **Sensitive Personal Data.** These data identify individuals by name, address, identifying number (e.g., Social Security Number), or other specific identifying information; and include information about the individual such as medical record, alcohol and drug abuse, sickle cell anemia, Human Immunodeficiency Virus (HIV) test or diagnosis data, financial transactions, education, criminal history, employment history, and familial relationships.

(2) **Sensitive Resource Data.** These data pertain to the control and distribution of funds or the diversion of economically valuable assets (e.g., supplies, controlled substances).

(3) **Mission-Critical Data.** These are data that if compromised could affect the accomplishment of a VA mission. Hard copy program listings and associated documentation are considered mission-critical.

(4**) Investigative Data.** These are data that include, but are not limited to audits and investigations, Quality Assurance audits and studies, risk analysis questionnaires, and health care facility computer audit trails and logs.

(5) **Contract Data.** Proprietary data used by the VA concerning specifications, Request for Procurement (RPFs), and the award of contracts are sensitive data.

(6) **Data, Text, and Images that Require Protection.** This includes any material not covered by other categories and that if compromised could result in fraud, theft or misappropriation of funds, and if misused could result in life threatening situations or adversely affect the delivery of health care.

b**. Transmission of Data, Text, and Images.** Depending upon the sensitivity of the material, different protective mechanisms may be used such as line protection devices or encryption/decryption procedures. The risk analysis process should include a determination if such protective mechanisms are necessary. **NOTE:** *In a local hospital environment, encryption should not be necessary.*

c. **Protection of Back-up Data.** In the event of loss of on-line data, provisions must be made to restore those databases with absolutely minimal loss of data. The Chief, IRM Service, shall ensure policies and procedures be in place to address data archival and protection of archived records.

d. **Data Access Controls.** The access controls which limit file-level access to sensitive data by system users should be established and documented for each sensitive system.

e. **Implementation of Data Security**

(1) VHA facility management shall ensure that appropriate data security features (e.g., system-determined number of log-on attempts, screen time-outs) are utilized, which in conjunction with system and application software AIS security measures, will protect AIS sensitive data which may be electronically communicated, transferred, processed, or stored.

(2) Facility management shall ensure that procedures are established and used to identify and report actual and suspected breaches of AIS security. Refer to MP-5, Part I, Chapter 752, “Discipline and Adverse Actions,” for a listing of items covered in this category.

f. **Disposition of Printed Data, Forms, and Related Records.** Forms and other printed output produced by computer systems shall be evaluated for data sensitivity. Printed output containing sensitive data may require special handling such as labeling, storage in locked cabinets or desks, disposal of forms and carbons in special containers, accountability of ownership and destruction by shredding or other appropriate methods. As a related consideration, software capabilities may be used to control access to hard copy peripherals (e.g., printers).

16.08 PROCEDURES FOR SYSTEM ACCESS

a. Use of VHA information assets (hardware, software, and data) is restricted to those with a need for them in the performance of their duties. VHA facility management, or their designee(s), shall approve access to VHA AIS functions upon receipt of a written and/or electronic request from the office and/or unit supervisor. At a minimum, this request shall include the name, service, purpose for access, and access requirements. All approved requests shall be routed through the VHA facility ISO.

b. VHA facility management shall designate and record individuals authorized to issue access to AIS functions and data.

c. Procedures for managing, recording and monitoring who has access to sensitive AIS shall be implemented.

d. The Log-On-Bulletin feature displays a security awareness message each time a user logs-on. A minimum one line message stating, "MISUSE OF THIS SYSTEM OR INFORMATION CONTAINED IN THIS SYSTEM IS A FEDERAL CRIME" is recommended for display.

e. Access and Verify Codes (DHCP security passwords)

(1) Individual access and verify codes are mandated for DHCP access and each unique code pair shall be used by only one person. The only exception to this mandate is access to the DHCP "Demonstration" processing environment.

(2) DHCP verify codes shall be changed at least once every 90 days which is an adequate compromise between system security and manageability. Actual procedures shall be documented at the local level.

16.09 PROCEDURES FOR USER ACCESS

a. A reliable system for granting and revoking access to VHA data assets is required to establish user accountability. All DHCP user access will be granted through the Kernel security system. A system for maintaining access records for all users, including non-VHA users, shall be implemented. The facility Director is ultimately responsible for the sensitive data processed and stored on the facility AIS. The ISO must periodically review AIS access.

b. A VHA management official shall sponsor user access (for all users, including non-VHA users, and shall recommend access for issue by the Chief, IRM Service. A written and signed request for user access by management, or designee(s), constitutes management approval (sponsorship) to initiate a request for access to any sensitive AIS. **NOTE:** *Access will be granted all non-VA users only if the purpose for access meets criteria of the Privacy Act and VA Confidentially regulations and transfer.*

(1) Requests for access to remote systems and networks not under the VHA facility management control (e.g., Austin Automation Center, Integrated Data Communications Utility (IDUC)) shall be routed through the ISO prior to approval.

(2) Access requirements to information systems by auditors, consultants, representatives of hardware and software vendors, communications company employees, volunteers, work-study students, and other members of the general public shall meet or exceed those requirements established for VHA employees.

c. A representative (e.g., application coordinator, supervisor) of the sponsoring organization shall assist the user in completing a request for user access. When the request has been signed and approved, it will be forwarded through proper channels to the Chief, IRM Service, or designee, for access processing.

d. Distribution of access codes and application menus shall be controlled by the Chief, IRM Service, and may be delegated only to the facility ISO. In the event a user cannot be contacted directly to be issued access codes, those codes shall be delivered using the double envelope method. Access agreements shall contain the date, user and sponsor signatures and, at the minimum, the following statements:

"As an employee of the Veterans Health Administration (VHA), and as an authorized user of the computer systems of the Department of Veterans Affairs (VA), I will be given access privileges to Federal data and computer systems, especially computer systems within or accessible by VHA staff, to perform the duties of my job. I understand the following policies apply to these data and computer systems:

(1) I will safeguard the security code(s), (e.g., DHCP access and verify codes) given to me. I may use my access security codes in the performance of my official duties. I may not exceed the access authority provided by my security codes. I acknowledge that I am strictly prohibited from disclosing my security code(s) to anyone for any reason except to the facility Information Security Officer (ISO), VHA ISO or Regional ISO. This includes my family, friends, fellow workers, supervisors, and subordinates.

(2) I acknowledge that I am not to use anyone else's security code(s) to obtain access to VA or other Federal computer systems. I understand that I will be held accountable for all work performed or changes made to the system and/or databases under my security code(s) and that I am not to allow anyone else to access a computer system using my security code(s).

(3) I understand that all data to which I may obtain access is and will remain the property of VA. I understand that, as an employee, I have an obligation to protect data and information which the loss, misuse, or unauthorized modification of or unauthorized access to could adversely affect the conduct of VA or other Federal programs. Further, I am aware that information about individuals is confidential and must be protected by law and regulations from unauthorized disclosure.

(4) I understand that VA electronic mail is to be used for official government business only. I am not authorized to use electronic mail either for personal messages not related to the performance of my official duties or in lieu of personal telephone calls.

(5) I understand that the ISO and computer staff will monitor the amount, types and contents of messages sent by individuals on electronic mail, and that reports will be generated regularly about how electronic mail is used by individual employees, including myself.

(6) I understand that improper access to, or unauthorized modification or disclosure of data (obtained through the computer or otherwise) may subject me to the imposition of criminal penalties and/or disciplinary or adverse action, as appropriate, under VA employee conduct regulations. Similarly, if I exceed my computer system access authority or use that authority to engage in conduct outside the scope of my official duties, I may also be subject to disciplinary or adverse action, as appropriate, and criminal prosecution.

(7) I understand that I am not to use my access authority to a VA or other federal computer system, particularly electronic mail, for any purpose other than performance of my official duties. Specifically, I may not access, disclose or change data except as authorized by VHA officials, including my supervisor, ISO, and computer staff.

(8) I understand that I may have disciplinary or adverse action, as appropriate, taken against me and may be prosecuted if I use electronic mail for any purpose other than performance of VA business within the scope of my official duties.

(9) I affirm that I have read and understand the provisions and intent of this notice and the importance of preserving computer access security.

(10) Unless and until I am released in writing by an authorized representative of the Department of Veterans Affairs, I understand that all conditions and obligations imposed upon me by this notice apply during the time I am granted access to a VA or other Federal computer system and at all times thereafter."

e. Procedures will be established that require all users to sign an "Access Agreement" before actual computer access is granted. The "Access Agreement" should state at a minimum that the user has reviewed and will abide with the facility's security policies and procedures. The signed access agreement will be maintained by the Chief, IRM Service, or delegated to the ISO.

f. Procedures shall be in place to review user change of status (e.g., transfer, termination, separation). Action shall be taken to ensure:

(1) The ISO, or designee, is included as part of the facility clearance process;

(2) The employee no longer has possession of unneeded sensitive data media;

(3) The employee has returned all keys and access devices;

(4) Employee security codes, electronic signatures, menu options, and security keys have been reviewed for either alteration or termination;

(5) IRM service chiefs are informed in an appropriate and timely manner;

(6) The supervisor debriefs the employee discussing the regulations on safeguarding sensitive data to ensure nondisclosure to any unauthorized persons or agencies; and

(7) The OIG is notified if an employee leaves a position requiring a sensitivity level designation (refer to subpar. 16.05e).

g. Programmer access to DHCP must be approved by VHA facility management, or their designee(s), and included on the user access list.

16.10 PROCEDURES FOR PHYSICAL SECURITY

a. **Environment.** Physical security addresses the environment of the computer system, such as construction features, physical access controls, and other measures used to protect computer resources from theft, vandalism, deliberate corruption of data, accidents, loss of utilities, and natural hazards (e.g., fire, flood).

(1) Physical security measures protect and preserve assets by reducing exposure to various threats.

(2) Staff and equipment must be afforded a safe, secure, and technically sound physical environment. While it is necessary to comply with each of the areas addressed, appropriate adjustments or allowances can be made for the organization, physical plant, and any special requirements of the individual facility.

(3) Facility management shall ensure procedures are established for identifying and reporting suspected or actual breaches of physical security. (Refer to the Federal Information Processing Standards (FIPS) Publication 31.)

b. **Peripheral and Communications Devices and Microcomputers.** Security measures shall be taken to protect against theft and unauthorized use of AIS peripheral and communications devices, microcomputers, and related items such as printers, floppy disks, and software.

(1) Remote off-site (e.g., dial-in) access to the computer system may be authorized locally. The removal of peripheral or communication devices from a facility for use off-site shall be controlled. Property passes shall be issued and a record shall be maintained of all AIS equipment and software removed from the facility, including the individual responsible for the equipment and the date(s) the equipment was removed from and returned to the facility.

(2) All physical security requirements (e.g., key and combination lock hardware, security surveillance television equipment, room intrusion detectors), as identified in the risk analysis, which may be deemed necessary by the facility IRM to protect peripheral devices and microcomputers, should be compatible with and, when possible, integrated into the host site security system.

(3) Access to storage media containing sensitive data shall be controlled by locks and access control procedures.

c. **Disposition of Forms and Related Records.** Forms and other types of printed output produced by computer system(s) shall be evaluated for data sensitivity and handled in accordance with Procedures for Security of Sensitive Data (see par. 16.07).

16.11 PROCEDURES FOR TECHNICAL SECURITY

Technical security procedures and mechanisms address the protection of sensitive data and programs, and the processing system. The procedures apply to information processing in mini and mainframe computers and microcomputers, office automation systems, and associated peripherals for these systems, and to storage media and telecommunications equipment. Chapters 8, 9, and 12, address MIRMO policy for development, testing, and distribution of software packages sent to health care facilities.

a. **Software Security.** The software protection mechanisms which prevent unauthorized access to system programs or data must address the selection of the system software protection and the administrative procedures used to implement the software.

(1) **Selection of Software**

(a) Unless centrally provided, the system software packages and routines for use in VHA AIS systems shall be identified and reviewed by Chief, IRM Service, as appropriate, prior to implementation. Site-specific characteristics of the system, such as its operating environment and other details, should be considered when deciding which of these packages or routines will be used and how the individual features of the selected system software will be implemented.

(b) IRM Chiefs shall consider the potential for infection with malicious code in the software being considered for procurement or use. No personally owned software shall be used on VHA information systems before it is tested and approved by the IRM Chief. Software shall be tested to ensure proper ownership, functionality, and that it is free of malicious code, (e.g., viruses, Trojan horses).

(2) **Security Software Features.** Based on the vulnerabilities and threats identified by the risk analysis, the following system security software features should be considered for use:

(a) **DHCP Access Code and/or Verify Code Protection.** Access codes, a unique set of at least 6 characters, are assigned to all system users. A unique verify code, also a unique set of 6 or more characters, is provided along with each access code.

(b) **Log-On Dialogue.** A feature which identifies a valid system user (one who has typed in a valid code) and directs the user to authorized options or applications (such as predefined in the DHCP User Authorization File). Use of such a feature limits user access and protects system programs and data files from unauthorized access.

(c) **Log-On Bulletin.** A security awareness message displayed each time a user logs on. A message of at least one line stating, "MISUSE OF THIS SYSTEM OR INFORMATION CONTAINED IN THIS SYSTEM IS A FEDERAL CRIME" is recommended for display.

(d) **File Protection.** File protection features provide the capability to limit the types of operations (e.g., read, write, delete, Data Dictionary modification) that can be performed by individual users on given data or program files.

(e) **Menu Management.** Menu management software limits the functions which can be accessed by a system user. This mechanism provides the system user with a menu of functions which the user is authorized to perform but prohibits access to other functions and thus provides program and file protection.

(f) **Personal Authentication Devices (PADs).** Devices are available which control system access through some form of "personal identification." These devices range from badge readers to very sophisticated smart cards to devices which can recognize user biometrics.

(g) **System Access, Transaction Logging, and Audit Trails.** The logging feature provides the capability to record actual or attempted access to the system and other activity. Information contained in such a log may include user name, log-on/log-off time, terminal location, files accessed, and transactions executed. Logging software provides valuable information for both system management and information security management.

(h) **Time-out Features.** Certain system software provides the capability to terminate a process automatically and log-off a user when an access session remains inactive for some specified length of time. For example, DHCP work station time-out feature should be set for a maximum of 3 minutes when sensitive data are being accessed in a location that is not physically secure.

(i) **Log-off Features.** A break of connection would cause immediate termination of an access session and a log-off shall immediately break the connection.

(j) **Integrity Checking Features.** These features (e.g., checksum program integrity checkers) included in application programs provide the capability of identifying the existence of program and/or system discrepancies.

(3) **Software Security Implementation Procedures.** Software designed to provide information security is limited by the effectiveness of the procedures implemented to support it. Procedural issues, which relate to the use of the system software and which should be addressed, are as follows:

(a) A minimum length of six characters is required for access and verify codes. The minimum length will be software controlled.

(b) Default User Accounts. Operating systems are sometimes installed with a standard set of default user accounts and associated standard security passwords. The access route shall be protected by either disabling the standard user account or by changing the passwords.

b. **Processing Environments.** VHA automated information systems use several processing environments which meet the specific and varied needs of users. Descriptions of processing environments and the unique aspects relating to information security for each follows.

(1) **Production.** Production is the environment for the processing of official data utilized in the provision of health services to the veteran, in support of regional management, and in support of facility missions. Facility information security procedures for production environments shall specifically address controls for:

(a) Viewing, modifying, downloading, or deleting production system data and programs,

(b) Generation and disposition of outputs,

(c) Tracking production program version changes (maintenance of a software update history log is recommended), and

(d) Access to the computer and its peripheral devices.

(2) **Development and Verification.** Development and verification is the environment for the development, testing, and verification of program code for the maintenance, modification or enhancement of existing applications, or the development of new applications. Information security procedures for this environment shall specifically address controls for:

(a) Viewing, modifying, or deleting test data;

(b) Creating, viewing, modifying, or deleting development programs;

(c) Generation and disposition of outputs;

(d) Transfer of application programs and data files from the development and verification environment to the production environment; and

(e) The computer system and its peripheral and telecommunication devices.

(3) **Demonstration and/or Training.** The demonstration and/or training environment enables use of system or application software functions in an on-line mode (using production or development computer resources) without affecting the production or development environments. The demonstration and/or training environment shall simulate on a demonstration or training disk, the production environment and use non-sensitive data to test, train, or demonstrate the system. Information security procedures for this environment shall specifically address:

(a) Protecting production and development system programs and data files;

(b) Accessing the "Demonstration" account by the general public (other than VHA staff);

(c) Limiting user access to only those capabilities necessary to utilize the demonstration programs; and

(d) Limiting access to the computer and its peripheral and communications devices. **NOTE:** *Generic access codes may be used to enter the "Demonstration" environment and is the only exception to the mandated requirement for individual password codes.*

c. **System Support Procedures.** Effective management of a computer system requires that system support procedures be established on a regular basis (e.g., daily, weekly, monthly).

(1) Each Chief, IRM Service, shall establish procedures to ensure the data required for contingency planning is current. Examples of data to be maintained by these procedures are the most frequently used manager routines, current software, and AIS application functions ranked by priority relative to the mission of the facility.

(2) Maintenance contracts commit hardware vendors to perform periodic preventive maintenance on computer systems. The Chief, IRM Service, shall ensure that a satisfactory preventive maintenance schedule is established and that the service adheres to that schedule.

(3) Facility management shall establish procedures to ensure IRM service chiefs maintain accountability for their systems, in accordance with M-11, Chapters 4 and 9. Each system installation of locally-developed software shall be reviewed and approved by the Chief, IRM Service, or designee, prior to installation.

(a) There shall be no local modification of the DHCP Kernel security software features.

(b) Willful and intentional modification of VHA software processing fiduciary data for illegal or disruptive purposes or for purposes of personal gain is a crime. There shall be no modifications of these programs except by the issuing ISC. The Chief, IRM Service, shall ensure the integrity and security of systems and data bases with the use of security, capacity, and performance monitors. For additional information, refer to M-11, Chapter 17.

d. **Facility Technical Security Requirements.** VHA facility management shall ensure:

(1) In concert with the total AIS Security Program, that adequate software security access to AIS is limited to authorized users.

(2) That procedures are developed and implemented and are applicable to the software security features selected for use on the facility AIS.

(3) That procedures are established for identifying and reporting actual or suspected breaches of software security.

(4) All technical security procedures shall be reviewed annually by the Chief, IRM Service, or systems manager, and modified as appropriate.

(5) The facility Chief, IRM Service, systems managers, and unit supervisors shall periodically review access restrictions to their computer system environments.

(6) That procedures are developed and implemented to provide software accountability for all facility computer systems, to include all small computers.

e. **Telecommunications and Networks.** VHA facility management shall implement the necessary mechanisms and procedures to protect information processed on networks, to include:

(1) Maintaining a record of authorized users of a network and their network privileges and reviewing this record on a regular basis to ensure that access to the network is limited to those individuals with a need to process;

(2) Ensuring that all networks are included in the facility risk analysis and contingency plan;

(3) Ensuring that computer systems are configured to terminate a user process if that user-network connectivity is interrupted before a proper log out;

(4) Ensuring that the network and systems automatically terminate sessions after periods of inactivity;

(5) Establishing formal reporting procedures for unexpected events and activity; and

(6) Ensuring for those networks not under VHA control, that when transmitting or receiving sensitive data, the networks meet the same criteria required of VHA networks.

16.12 PROCEDURES FOR CONTRACTOR/PROCUREMENT SECURITY

All technical, administrative, physical, and personnel security requirements shall be included in specifications for the acquisition or operation of information technology installations, equipment, software, and related services, whether procured by the agency or by the General Services Administration (GSA). Each VHA facility shall ensure that computer system contract documents for all outside services (contractors and maintenance personnel) and system users under authorized information resource procurement and sharing agreements, include a written requirement stating that they (e.g., contractor) meet the minimal security clearance levels defined in paragraph 16.05, Procedures for Personnel Security Management. **NOTE:** *Access to VHA information resource assets by non-VA staff is described in paragraph 16.09, Procedures for User Access.*

a. **Contractor Personnel Security**

(1) Security requirements and specifications for hardware and software maintenance personnel contracted from commercial sources shall be defined and approved prior to the signing of contractual agreements.

(a) The security implications of using non-VA maintenance personnel shall be considered when determining the security requirements for AIS.

(b) Such requirements will vary depending upon the level of trust associated with the equipment or system to be maintained.

(c) Contracts should stipulate that the contractor is responsible for the cost of background investigations, if required.

(2) Maintenance contractors and their employees shall be granted limited and controlled access to computer equipment and systems consistent with established security requirements. The procedures specified in Procedures for Personnel Security Management (see par. 16.05) and Procedures for User Access (see par. 16.09) shall be followed.

(3) Procurement officials for all VHA facilities shall ensure negotiated contracts pertaining to AIS services include a separate section dealing with information security issues specifying the level of trust required and contractor responsibility in complying with established requirements.

b. **Contractor Security and/or RFP Review**

(1) Procurement officials for all VHA facilities shall ensure that all RFPs and purchase agreements pertaining to AIS hardware and software are reviewed for security implications. Such officials are responsible for the inclusion of a separate section in the contract dealing with information security issues, where appropriate.

(2) The ISO shall advise the procurement official if security specifications are adequate or need strengthening.

(3) All computer system contractors shall be required to meet the minimal security requirements defined in paragraph 16.05, Procedures for Personnel Security Management.

c. Computer System Sharing Agreements

(1) All non-VA users having access to VA information resources through a negotiated sharing agreement shall meet the minimum security clearance levels defined in paragraph 16.05, Procedures for Personnel Security Management, prior to the effective date of the agreement. The organization

requesting access to VA resources shall bear the responsibility of ensuring that security requirements are included in the written agreement and that they are met.

(2) Approving officials shall ensure that all information resource sharing agreements pertaining to computer hardware and software are reviewed for security implications. Such officials are responsible for the inclusion of a separate section in the agreement dealing with information security issues, as appropriate.

16.13 PROCEDURES FOR AIS SECURITY PROGRAM ASSESSMENT

The VHA Information Security Program is subject to review for compliance with Federal, Departmental, and VHA standards. Assessment is required to ensure that the Information Security Program in each facility actively encompasses each of the key program elements described in this chapter. The MIRMO MISS has the role of assessing all administrative and technical aspects of the Information Security Program. Other organizations may include review of information security programs as part of their general review of the facility or inspection of information systems.

a. **VHA Assessments**

(1) **Internal Assessment**

(a) The VHA facility shall complete their facility assessments at least every 2 years, on or before the anniversary date of the first internal assessment which occurred during 1988. The facility ISO shall participate in this effort.

(b) The assessment shall be based, at a minimum, on AIS Program requirements, as well as OMB Circular A-123.

(c) Results of the self-assessment and any recommendations shall be submitted to the VHA facility Director for review and any indicated action.

(d) The response of the facility Director to the facility self-assessment shall be completed within 1 month after the completion of the assessment and given to the Chief, IRM Service, or systems manager to follow-up for corrective actions.

(e) The assessment, response, and correspondence related to these assessments shall be considered sensitive data. The Chief, IRM Service, or systems manager and director shall ensure the confidentiality of the contents of the self-assessment report. The self-assessment shall be documented in a report marked "sensitive" and attached to VA Form 0230, Sensitive Document Cover.

(f) The self-assessment shall be maintained at the VHA facility in a secure file and available for review by the ISO, RISO, and other authorized individuals (e.g., Joint Commission on the Accreditation of Healthcare Organizations (JCAHO), OIG).

(g) The document shall not be distributed to other than authorized personnel.

(2) **External Assessment**

(a) External assessment of each VHA facility will be conducted on a 5-year cycle (refer to MP-6, Pt. I, chg. 15).

(b) Staff from the NCIS will participate in information security program assessments of local facilities, and RISOs may participate in these assessments or chair external assessment teams. The RISOs shall

support external assessment activities in conjunction with each facility Director and ISO and the staff at the NCIS.

(c) The assessment shall be based on AIS security program requirements, as well as other applicable information security Federal laws and regulations (see App. 16A).

(d) Personnel performing an external assessment shall consider the assessment written results as a sensitive document. Results should be viewed on a need-to-know basis only. A copy of the report shall be sent, using the double envelope method, to the Director, MISS, VA Central Office. The RISO shall keep one copy in a secure file.

(e) The assessment results will be reported only to the Director of the facility and the applicable Regional Director (RD) within 3 weeks of its completion. The report shall be mailed to the facility Director and the RD using the double envelope method.

(f) The facility Director shall respond to the RD and the Director, MISS, concerning the assessment within 1 month after the receipt date of the external assessment documents. The assessments and comments are sensitive documents and their distribution shall be kept limited.

(g) The Director, MIRMO, will provide a summary report of external assessment annually to the Under Secretary for Health.

b. **Assessments by Other Organizations** (e.g., the VA Inspector General, Government Accounting Office). The information security programs in all VHA facilities will be subject to review for compliance by agency, department, and Federal oversight organizations. Should policy conflicts arise during these reviews, the policy having the most stringent requirements shall apply.

16.14 PROCEDURES FOR RISK ANALYSIS

a. A program for the conduct of periodic risk analyses at each installation shall be established and maintained to ensure that appropriate, cost-effective safeguards are incorporated into existing and new installations.

(1) The objective of a risk analysis is to provide a measure of the relative vulnerabilities and threats to an installation so that security resources can be effectively distributed to minimize potential loss.

(2) There are two general types of risk analyses to be conducted. One for the overall facility and another for each AIS operated by, or on behalf of the facility.

(3) The results of these analyses should be documented and taken into consideration by management officials when certifying sensitive applications processed at the installation. Not all risk can be avoided. Budget constraints, staffing limitations, cost-benefit considerations (controls can cost more than potential losses) may result in the acceptance of certain existing risks.

(4) A risk analysis shall be performed not less than every 2 years.

b. VHA facility management shall ensure that a complete risk analysis is performed at least every 2 years and is documented in a risk analysis report.

(1) This sensitive report shall be protected and covered with VA Form 0230. The risk analysis shall use the criteria provided in the Facility Risk Analysis Questionnaire and AIS Risk Analysis Questionnaire. **NOTE:** *Copies of the questionnaires may be obtained from MISS, MIRMO.*

(2) Vulnerabilities found during any analysis shall be corrected or accepted as uncontrolled risks by the facility Director. If the decision is to accept a risk, this decision shall be documented as an uncontrolled

risk and signed by the facility Director. This sensitive document shall be maintained by the Chief, IRM Service, or designee, along with the risk analysis report and shall be available for review by authorized reviewing organizations (e.g., RD).

c. The risk analysis questionnaire and associated correspondence shall be considered sensitive documents and appropriately labeled, handled, and filed in a locked cabinet. The document(s) shall have VA Form 0230, permanently attached over the first page. Sensitive data are described in greater detail in paragraph 16.07, Procedures for Security of Sensitive Data.

d. A Facility Risk Analysis Questionnaire is intended for completion by the facility every 2 years. It focuses on potential facility-level risks. The AIS Risk Analysis Questionnaire is intended for completion by the Chief, IRM Service, or designee, for each AIS within the facility. It focuses on potential vulnerability and shall be addressed.

(1) The Chief, IRM Service, or designee, shall review the questionnaires for completeness and assess the magnitude of the risks to the facility.

(2) The Chief, IRM Service, or designee, shall retain the questionnaires, cover with VA Form 0230, and store in a locked enclosure.

e. Facility management shall develop plans for correcting known vulnerabilities.

(1) The plans shall include specific tasks and schedules with target dates.

(2) All specific plans concerning security shall be considered sensitive information and labeled appropriately, covered with VA Form 0230, and stored in a secured location when not in use.

16.15 AIS CONTINGENCY MANAGEMENT

Policies shall be established and responsibilities assigned to ensure that appropriate contingency plans are developed and maintained for each facility AIS. Such plans should be consistent with disaster recovery and continuity of operations plans maintained by the VHA facility at which the application is processed, and shall be developed in accordance with OMB Circular A-130. At a minimum, the contingency plan will address the following:

a. Procedures to cover the appropriate emergency response to fire, flood, civil disorder, natural disaster, bomb threat, or any other incident or activity, to protect lives, limit damage, and minimize the impact on data processing operations.

b. Procedures to ensure that essential business functions (e.g., medical, administrative, accounting) can be conducted after disruption of the facility and/or user processing capability.

c. Procedures necessary to rapidly restore the facility and/or user processing capability following physical destruction, major damage, or loss of data.

16.16 CERTIFICATION AND RECERTIFICATION

After systems testing of all new applications and of significant modifications to existing applications, an agency official shall certify that the system meets all applicable Federal policies, regulations and standards, and that the results of the tests demonstrate that the installed security safeguards are adequate for the application.

a. Agencies are required to conduct periodic audits or reviews of sensitive applications and recertify the adequacy of security safeguards. Audits or reviews and recertification shall be performed at least every 3 years.

b. Audits or reviews and recertification are considered a part of agency vulnerability assessments and internal control reviews. OMB required certification/recertification of centrally-managed systems (e.g., DHCP) is the responsibility of the Under Secretary for Health, or designee.

REFERENCES

1. Title 5 United States Code (U.S.C.) 552, "Freedom of Information Act," c. 1967

2. Title 5 U.S.C. 552a, "Privacy Act," c. 1974, as amended

3. Title 5 U.S.C. Sections 7361 and 7362, "Confidentiality of employee records concerning substance abuse prevention, treatment or rehabilitation"

4. Title 18 U.S.C. 1030, "Fraud and related activity in connection with computers"

5. Title 18 U.S.C. 2510, "Electronic Communications Privacy Act of 1986"

6. Title 18 U.S.C. Section 2701, "Unlawful access to stored communications"

7. Title 38 U.S.C. 901-905, "Security and law enforcement on property under the jurisdiction of the Veterans Administration"

8. Title 38 U.S.C. 5701, "Confidential nature of claims"

9. Title 38 U.S.C. 5705, "Confidentiality of medical quality - assurance records"

10. Title 38 U.S.C. 7332, "Confidentiality of certain medical records," as amended

11. Title 44 U.S.C. Chapter 35, "Paperwork Reduction Act," as amended

12. Public Law No. 100-235, 101 Stat 1724 (1988), "Computer Security Act of 1987"

13. Title 38 Code of Federal Regulations (CFR) 1.500 through 1.527 and 1.575 through 1.584

14. Title 42 CFR 2.1 through 2.67

15. Office of Management and Budget (OMB) Circulars and Bulletins:

    a. A-123, "Internal Control Systems"

    b. A-127, "Financial Management Systems"

    c. A-130, "Management of Federal Information Resources"

    d. OMB Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information"

    e. OMB Memorandum M-88-10, "Model Framework for Management Control Over Automated Information Systems"

16. Federal Information Processing Standards (FIPS):

    a. Publication 31, "Guidelines for Automatic Data Processing Physical Security and Risk Management"

    b. Publication 39, "Glossary for Computer Systems Security"

c. Publication 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974"

d. Publication 46, "Data Encryption Standards"

e. Publication 48, "Guidelines on Evaluation for Automated Personnel Identification"

f. Publication 65, "Guidelines for Automatic Data Processing Risk Analysis"

g. Publication 73, "Guidelines for Security of Computer Applications"

h. Publication 81, " Data Encryption Standards (DES) Modes of Operation"

i. Publication 83, "Guideline On User Authentication Techniques for Computer Network Access Control"

j. Publication 87, "Guidelines for ADP Contingency Planning"

k. Publication 88, "Guidelines on Integrity Assurance and Control in Database Administration"

l. Publication 102, "Guidelines for Computer Security Certification and Accreditation"

m. Publication 112, "Standard on Password Usage"

17. Federal Personnel Manual (FPM):

a. Chapter 731, "Personnel Suitability"

b. Chapter 731, Subchapter 4; FPM Letter 292-39

c. Chapter 732,, "Personnel Security"

d. Chapter 736, "Personnel Investigations"

e. Chapter 754, "Suitability Disqualification Actions"

18. Department of Veterans Affairs (VA) Manuals

a. MP-1, Part I, Chapter 2, "Center Security and Law Enforcement"

b. MP-1, Part I, Chapter 5, "Security"

c. MP-1, Part II, Chapter 13, "Emergency Preparedness Planning"

d. MP-5, Part I, Chapter 294, "Availability of Official Information"

e. MP-5, Part I, Chapter 297, "Protection of Privacy in Personnel Records"

f. MP-5, Part I, Chapter 735, Employee Responsibilities and Conduct" and 38 CFR 800 on rules of conduct

g. MP-5, Part I, Chapter 752, Appendix C, "Tables of Examples of Offenses and Penalties"

h. MP-6, Part I, Chapter 2, "Automated Information Systems Security"

I. M-1, Part I, Chapter 9, “Release of Medical Information.”

19. Department of Defense (DOD) Standard 5200.28, "Department of Defense Trusted Computer System Evaluation Criteria"